Amendments to the Claims

Claim 1 (currently amended): A computer program product for efficiently generating pseudo-random bits, the computer program product embodied on one or more computer readable media and comprising:

computer-readable program code means for providing an input value;

computer-readable program code means for generating an output sequence of pseudo-random bits using the provided input value as an exponent of ~~input to~~ a 1-way function comprising modular exponentiation modulo a safe prime number, wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and a base of the modular exponentiation is a fixed generator value; and

computer-readable program code means for using C selected bits of the generated output sequence as the provided input value for a next iteration of the computer-readable program code means for generating while using all N - C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.

Claim 2 (original): The computer program product according to Claim 1, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 3 - 5 (canceled)

Claim 6 (currently amended): The computer program product according to Claim [[4]] 1, wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

Claim 7 (original): The computer program product according to Claim 1, wherein the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 8 (canceled)

Claim 9 (previously presented): The computer program product according to Claim 1, wherein the N - C remaining bits are concatenated to pseudo-random output bits previously generated by the computer-readable program code means for generating.

Claim 10 (previously presented): The computer program product according to Claim 1, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as a contiguous group of bits.

Claim 11 (previously presented): The computer program product according to Claim 1, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as a non-contiguous group of bits.

Claim 12 (previously presented): The computer program product according to Claim 1, further comprising computer-readable program code means for using the desired number of generated pseudo-random bits as input to an encryption operation.

Claim 13 (currently amended): A system for efficiently generating pseudo-random bits in a computing environment, comprising:

means for providing an input value;

means for generating an output sequence of pseudo-random bits using the provided input value as an exponent of ~~input to~~ a 1-way function comprising modular exponentiation modulo a safe prime number, wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and a base of the modular exponentiation is a fixed generator value; and

means for using C selected bits of the generated output sequence as the provided input value for a next iteration of the means for generating while using all N - C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.

Claim 14 (original): The system according to Claim 13, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 15 - 17 (canceled)

Claim 18 (currently amended): The system according to Claim [[16]] 13, wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

Claim 19 (original): The system according to Claim 13, wherein the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 20 (canceled)

Claim 21 (previously presented): The system according to Claim 13, wherein the N - C remaining bits are concatenated to pseudo-random output bits previously generated by the means for generating.

Claim 22 (previously presented): The system according to Claim 13, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as a contiguous group of bits.

Claim 23 (previously presented): The system according to Claim 13, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as a non-contiguous group of bits.

Claim 24 (previously presented): The system according to Claim 13, further comprising means for using the desired number of generated pseudo-random output bits as input to an encryption

operation.

Claim 25 (currently amended): A method for efficiently generating pseudo-random bits, comprising the steps of:

providing an input value;

generating an output sequence of pseudo-random bits using the provided input value as an exponent of ~~input to~~ a 1-way function comprising modular exponentiation modulo a safe prime number, wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and a base of the modular exponentiation is a fixed generator value; and

using C selected bits of the generated output sequence as the provided input value for a next iteration of the generating step while using all N - C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.

Claim 26 (original): The method according to Claim 25, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 27 - 29 (canceled)

Claim 30 (currently amended): The method according to Claim [[28]] 25, wherein the length of the input value is at least 160 bits and a length of the safe prime number is at least 1024 bits.

Claim 31 (original): The method according to Claim 25, wherein the length of the input value is 160 bits and the length of the generated output sequence is 1024 bits.

Claim 32 (original): The method according to Claim 25, wherein the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

Claim 33 (canceled)

Claim 34 (previously presented): The method according to Claim 25, wherein the N - C remaining bits are concatenated to pseudo-random output bits previously generated by the generating step.

Claim 35 (previously presented): The method according to Claim 25, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as a contiguous group of bits.

Claim 36 (previously presented): The method according to Claim 25, wherein the N - C remaining bits are selected from the N bits of the generated output sequence as a non-contiguous group of bits.

Claim 37 (previously presented): The method according to Claim 25, further comprising the step

of using the desired number of generated pseudo-random output bits as input to an encryption operation.

Claim 38 (canceled)

Claim 39 (currently amended): An encryption system, comprising:

means for providing an input value;

means for generating an output sequence of pseudo-random bits using the provided input value as an exponent of ~~input to~~ a 1-way function comprising modular exponentiation modulo a safe prime number, wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and a base of the modular exponentiation is a fixed generator value;

means for using C selected bits of the generated output sequence as the provided input value for a next iteration of the means for generating while using all N - C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated; and

means for using the desired number of generated pseudo-random bits as input to an encryption operation.

Claim 40 (original): The encryption system according to Claim 39, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 41 - 43 (canceled)

Claim 44 (currently amended): The encryption system according to Claim [[42]] 39, wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

Claim 45 (original): The encryption system according to Claim 39, wherein the length of the input value is 160 bits and the length of the generated output sequence is 1024 bits.

Claim 46 (canceled)

Claim 47 (previously presented): The encryption system according to Claim 46, wherein the N - C remaining bits arc concatenated to pseudo-random output bits previously generated by the means for generating.